CODE BREAKERS OF ROOM 40

Cryptography, or the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography, that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids.

In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma Rotor Machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper.

The development of cryptography has been paralleled by the development of cryptanalysis — the "breaking" of codes and ciphers. The discovery and application, early on, of frequency analysis to the reading of encrypted communications has, on occasion, altered the course of history.

The earliest known use of cryptography is found in non-standard hieroglyphs carved into monuments from the Old Kingdom of Egypt circa 1900 BCE. These are not thought to be serious attempts at secret communications, however, but rather to have been attempts at mystery, intrigue, or even amusement for literate onlookers.

These are examples of still other uses of cryptography, or of something that looks (impressively if misleadingly) like it. Some clay tablets from Mesopotamia somewhat later are clearly meant to protect information —one dated near 1500 BCE was found to encrypt a craftsman's recipe for pottery glaze, presumably commercially valuable. Later still, Hebrew scholars made use of simple mono-alphabetic substitution ciphers (such as the Atbash cipher) beginning perhaps around 500 to 600 BCE.

A Scytale, an early device for encryption.

The ancient Greeks are said to have known of ciphers. The scytale transposition cipher was used by the Spartan military, however it is disputed whether the scytale was for encryption, authentication, or avoiding bad omens in speech.

Herodotus tells us of secret messages physically concealed beneath wax on wooden tablets or as a tattoo on a slave's head concealed by regrown hair, though these are not properly examples of cryptography *per se* as the message, once known, is directly readable; this is known as steganography. Another Greek method was developed by Polybius (now called the "Polybius Square"). The Romans knew something of cryptography (e.g., the Caesar cipher and its variations).

Although cryptography has a long and complex history, it wasn't until the 19th century that it developed anything more than ad hoc approaches to either encryption or cryptanalysis (the science of finding weaknesses in crypto systems). Examples of the latter include Charles Babbage's Crimean War era work on mathematical cryptanalysis of poly-alphabetic ciphers, redeveloped and published somewhat later by the Prussian Friedrich Kasiski.

Edgar Allan Poe used systematic methods to solve ciphers in the 1840s. In particular he placed a notice of his abilities in the Philadelphia paper Alexander's Weekly (Express) Messenger, inviting submissions of ciphers, of which he proceeded to solve almost all. His success created a public stir for some months.

He later wrote an essay on methods of cryptography which proved useful as an introduction for novice British cryptanalysts attempting to break German codes and ciphers during World War I, and a famous story, The Gold-Bug, in which cryptanalysis was a prominent element. Cryptography, and its misuse, were involved in the execution of Mata Hari and in the Dreyfus' conviction and imprisonment, Cryptographers were also involved in exposing the machinations which had led to the Dreyfus affair; Mata Hari, in contrast, was shot.

At the end of 1894 a French army captain named Alfred Dreyfus, a graduate of the Ecole Polytechnique and a Jew of Alsatian origin, was accused of handing secret documents to the Imperial German military. After a closed trial, he was sentenced to prison for life for treason and deported to Devil's Island. At that time, the opinion of the French political class was unanimously unfavourable towards Dreyfus.

Alfred Dreyfus

Certain of the injustice of the sentence, the family of the Captain, through his brother Mathieu, worked with the journalist Bernard Lazare to prove his innocence.

Meanwhile Colonel Georges Picquart, head of counter-espionage, found evidence in March 1896 indicating that the real traitor was Major Ferdinand Walsin Esterhazy. The General Staff, however, refused to reconsider its judgment and transferred Picquart to North Africa.

In July 1897 his family contacted the President of the Senate Auguste Scheurer-Kestner to draw attention to the fragility of the evidence against Dreyfus. Scheurer-Kestner reported three months later that he was convinced of the innocence of Dreyfus and also persuaded Georges Clemenceau, a former MP and then a newspaper reporter.

In the same month, Mathieu Dreyfus complained to the Ministry of War against Walsin-Esterhazy. While the circle of Dreyfusards widened, in January 1898 two nearly simultaneous events gave a national dimension to the case: Esterhazy was acquitted of treason charges (afterwards shaving his mustache and fleeing France), and Émile Zola published his "*J'Accuse* .!," a Dreyfusard declaration that rallied many intellectuals to Dreyfus' cause.

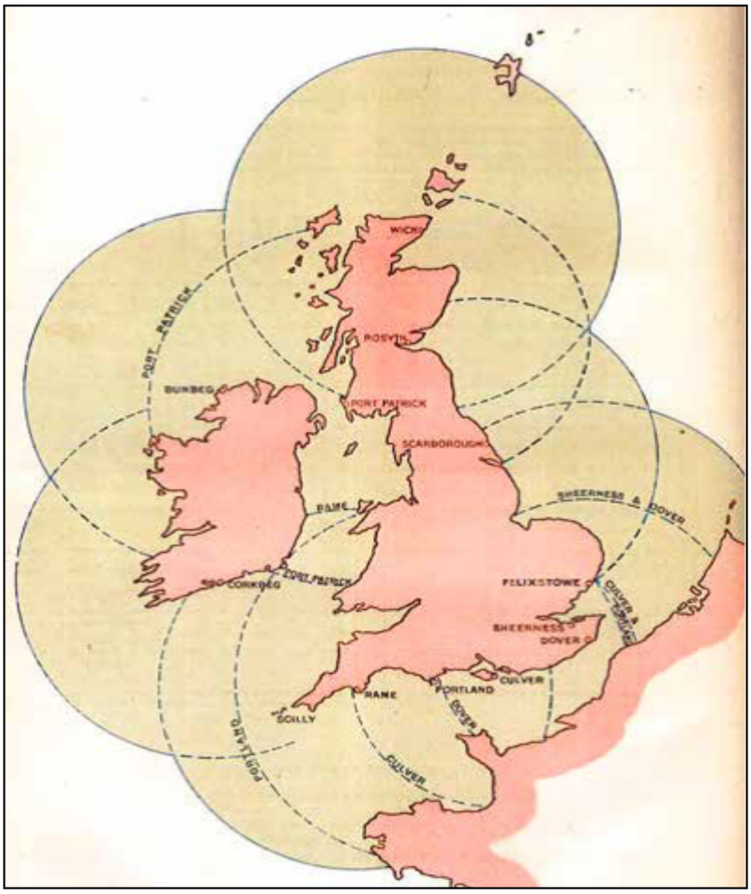
France became increasingly divided over the case, and the issue would continue to be hotly debated until the end of the century. Anti-semitic riots erupted in more than twenty French cities. There were several deaths in Algiers. The Republic was shaken, which prompted a sense that the Dreyfus Affair had to be resolved to restore calm and protect the stability of the nation.

Despite the intrigues of the army to quell the case, the first judgment against Dreyfus was annulled by the Supreme Court after a thorough investigation and a new Court Martial was held at Rennes in 1899. Despite increasingly robust evidence to the contrary Dreyfus was convicted again and sentenced to ten years of hard labour, though the sentence was commuted due to extenuating circumstances.

Exhausted by his deportation for four long years Dreyfus accepted the presidential pardon granted by President Émile Loubet. It was only in 1906 that his innocence was officially recognized through a decision without recourse by the Supreme Court. Rehabilitated, Dreyfus was reinstated in the army with the rank of Major and participated in the First World War. He died in 1935.

In 1911, a sub-committee of the Committee of Imperial Defence on cable communications concluded that in the event of war with Germany, German-owned submarine cables should be destroyed. In the early hours of 5 August 1914, the cable ship *Alert* located and cut Germany's five trans-Atlantic cables, which ran down the English Channel. Soon after, the six cables running between Britain and Germany were cut.

As an immediate consequence, there was a significant increase in cable messages sent via cables belonging to other countries, and cables sent by wireless. These could now be intercepted, but codes and ciphers were naturally used to hide the meaning of the messages, and neither Britain nor Germany had any established organisations to decode and interpret the messages. At the start of the war, the navy had only one wireless station for intercepting messages, at Stockton. However, installations belonging to the Post Office and the Marconi Company, as well as private individuals who had access to radio equipment, began recording messages from Germany.



Wireless Transmitter Low Power Shore Stations showing range with Royal Naval First Class Ships.

Intercepted messages began to arrive at the Admiralty intelligence division, but no one knew what to do with them. Rear-Admiral Henry Oliver had been appointed Director of the Intelligence division in 1913. In August 1914, his department was fully occupied with the war and no-one had experience of code breaking. Instead he turned to a friend, Sir Alfred Ewing, the Director of Naval Education (DNE), who previously had been a professor of engineering with a knowledge of radio communications and who he knew had an interest in ciphers.

It was not felt that education would be a priority during the expected few months duration of the war, so Ewing was asked to set up a group for decoding messages. Ewing initially turned to staff of the naval colleges Osborne andDartmouth, who were currently available, due both to the school holidays and to naval students having been sent on active duty.

Alastair Denniston had been teaching German but later became second in charge of Room 40, then becoming Chief of its successor after the First World War, the Government Code and Cypher School (located at Bletchley Park during the Second World War).

Others from the schools worked temporarily for Room 40 until the start of the new term at the end of September. These included Charles Godfrey, the Headmaster of Osborne (whose brother became head of naval Intelligence during the Second World War), two Naval instructors, Parish and Curtiss, and scientist and mathematician Professor Henderson from Greenwich Naval College.

Volunteers had to work at code breaking alongside their normal duties, the whole organisation operating from Ewing's ordinary office where code breakers had to hide in his secretary's room whenever there were visitors concerning the ordinary duties of the DNE.

Cdr Alexander Guthrie "Alastair" Denniston

Two other early recruits were R. D. Norton, who had worked for the Foreign Office, and Richard Herschell, who was a linguist, an expert on Persia and an Oxford graduate. None of the recruits knew anything about code breaking but were chosen for knowledge of German and certainty they could keep the matter secret.

A similar organisation had begun in the Military Intelligence department of the War Office, which become known as MI1b, and Colonel MacDonagh proposed that the two organisations should work together. Little success was achieved except to organise a system for collecting and filing messages until the French obtained copies of German military ciphers.

The two organisations operated in parallel, decoding messages concerning the Western Front. A friend of Ewing's, a barrister by the name of Russell Clarke, plus a friend of his, Colonel Hippisley, approached Ewing to explain that they had been intercepting German messages.

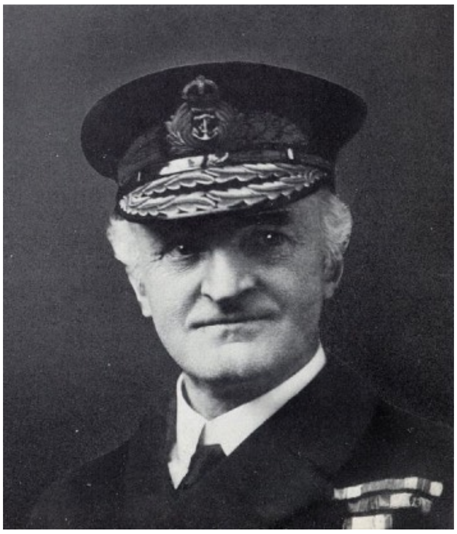
Ewing arranged for them to operate from the coastguard station at Hunstanton in Norfolk, where they were joined by another volunteer, Leslie Lambert (later becoming known as a BBC broadcaster under the name A. J. Alan).

Hunstanton and Stockton formed the core of the interception service (known as' Y' service), together with the Post Office and Marconi stations, which grew rapidly to the point it could intercept almost all official German messages. At the end of September, the volunteer schoolmasters returned to other duties, except for Denniston; but without a means to decode German naval messages there was little specifically naval work to do.

After hostilities commenced in August 1914 the Admiralty's secret intelligence unit, Room 40, stepped-up its monitoring and code breaking operations against Germany, providing the British armed forces with tide-turning information about the enemy's plans. Based in the Admiralty Building in London, it was in several ways a predecessor to the more concerted and sophisticated code-breaking operations at Bletchley Park during the Second World War.

Room 40's contribution to the war effort surveyed the role played by Admiralty intelligence in the lead-up to the declaration of hostilities in August 1914. Soon after this it became clear to all national combatants that the ability to adjust and change to meet new circumstances would define the winners and the losers.

In early November 1914 Captain William Hall, son of the first head of Naval Intelligence, was appointed as the new DID to replace Oliver, who had first been transferred to Naval Secretary to the First Lord and then Chief of the Admiralty War Staff. Hall had formerly been captain of the battlecruiser *Queen Mary* but had been forced to give up sea duties due to ill health. Hall was to prove an extremely successful DID, despite the accidental nature of his appointment.



Once the new organisation began to develop and show results it became necessary to place it on a more formal basis than squatting in Ewing's office. On 6 November 1914 the organisation moved to Room 40 in the Admiralty Old Building, which was by default to give it its name.

Room 40 has since been renumbered, but still exists in the original Admiralty Building off Whitehall, London, on the first floor, with windows looking inwards to a courtyard wholly enclosed by Admiralty buildings. Previous occupants of the room had complained that no one was ever able to find it, but it was on the same corridor as the Admiralty boardroom and the office of the First Sea Lord, Sir John Fisher, who was one of the few people allowed to know of its existence. Adjacent was the First Lord's residence (then Winston Churchill), who was another of those people.

William Reginald "Blinker" Hall, KCMG, CB, RN.

Others permitted to know of the existence of a signals interception unit were the Second Sea Lord, the Secretary to the Admiralty, the Chief of Staff (Oliver), the Director of Operations Division (DOD) and the assistant director, the Director of Intelligence Division (DID, Captain William Hall) and three duty captains. Admiral Sir Arthur Wilson, a retired First Sea Lord, had returned to the admiralty to work with the staff and was also included in the secret. The Prime Minister may also have been informed.

All messages received and decoded were to be kept completely secret, with copies only being passed to the Chief of Staff and Director of Intelligence. It was decided that someone from the intelligence department needed to be appointed to review all the messages and interpret them from the perspective of other information.

Rotter was initially suggested for the job, but it was felt preferable to retain him in code breaking and Commander Herbert Hope was chosen, who had previously been working on plotting the movements of enemy ships. Hope was initially placed in a small office in the west wing of the Admiralty in the Intelligence Section, and waited patiently for the few messages which were approved for him to see.

Hope reports that he attempted to make sense of what he was given and make useful observations about them, but without access to the wider information being received his early remarks were generally unhelpful. He reported to Hall that he needed more information, but Hall was unable to help.

On 16 November, after a chance meeting with Fisher where he explained his difficulties, Hope was granted full access to the information together with instructions to make twice daily reports to the First Sea Lord. Hope knew nothing of cryptanalysis or German, but working with the code breakers and translators he brought detailed knowledge of naval procedures to the process, enabling better translations and then interpretations of received messages. In the interests of secrecy, the intention to give a separate copy of messages to the DID was dispensed with so that only the Chief of Staff received one, and he was to show it to the First Sea Lord and Arthur Wilson.

As the number of intercepted messages increased, it became part of Hope's duties to decide which were unimportant and should just be logged, and which should be passed on outside Room 40. The German fleet was in the habit each day of reporting by wireless the position of each ship and giving regular position reports when at sea. It was possible to build up a precise picture of the normal operation of the High Seas Fleet, indeed to infer from the routes they chose where defensive minefields had been placed and where it was safe for ships to operate.

Whenever a change to the normal pattern was seen, it signalled that some operation was about to take place and a warning could be given. Detailed information about submarine movements was available. Most of this information, however, was retained wholly within Room 40 although a few senior members of the Admiralty were kept informed, as a huge priority was placed by the Staff upon keeping secret the British ability to read German transmissions.

Jellicoe, commanding the Grand Fleet, on three occasions requested from the Admiralty that he should have copies of the codebook which his cruiser had brought back to Britain, so that he could make use of it intercepting German signals. Although he was aware that interception was taking place, little of the information ever got back to him, or it did so very slowly.

No messages based upon Room 40 information were sent out except those approved by Oliver personally (except for a few authorised by the First Lord or First Sea Lord). Although it might have been impractical and unwise for code breaking to have taken place on board ship, members of Room 40 were of the view that full use was not being made of the information they had collected, because of the extreme secrecy and being forbidden to exchange information with the other intelligence departments or those planning operations.

Signals interception and direction finding

The British and German interception services began to experiment with direction-finding radio equipment in the start of 1915. Captain Round, working for Marconi, had been carrying out experiments for the army in France and Hall instructed him to build a direction-finding system for the navy.

At first this was sited at Chelmsford but the location proved a mistake and the equipment was moved to Lowestoft. Other stations were built at Lerwick, Aberdeen, York, Flamborough Head and Birchington and by May 1915 the Admiralty was able to track German submarines crossing the North Sea. Some of these stations also acted as 'Y' stations to collect German messages, but a new section was created within Room 40 to plot the positions of ships from the directional reports. A separate set of five stations was created in Ireland under the command of the Vice Admiral at Queenstown for plotting ships in the seas to the west of Britain and further stations both within Britain and overseas were operated by the Admiral commanding reserves.

The German navy knew of British direction-finding radio and in part this acted as a cover, when information about German ship positions was released for operational use. The two sources of information, from directional fixes and from German reports of their positions, complemented each other. Room 40 was able to observe, using intercepted wireless traffic from Zeppelins which were given position fixes by German directional stations to help their navigation, that the accuracy of British systems was better than their German counterparts. This was explainable by the wider baseline used in British equipment.

Room 40 had very accurate information on the positions of German ships but the Admiralty's priority remained to keep the existence of this knowledge secret. Hope was shown the regular reports created by the Intelligence Division about German ship whereabouts so that he might correct them. This practice was shortly discontinued, for fear of giving away their knowledge. From June 1915, the regular intelligence reports of ship positions were no longer passed to all flag officers, only to Jellicoe, who was the only person to receive accurate charts of German minefields prepared from Room 40 information.

Some information was passed to Beatty (commanding the battlecruisers), Tyrwhitt (Harwich destroyers) and Keyes (submarines) but Jellicoe was unhappy with the arrangement. He requested that Beatty should be issued with the *Cypher B* (reserved for secret messages between the Admiralty and him) to communicate more freely and complained that he was not getting sufficient information.

All British ships were under instructions to use radio as sparingly as possible and to use the lowest practical transmission power. Room 40 had benefited greatly from the free chatter between German ships, which gave them many routine messages to compare and analyse, and from the German habit of transmitting at full power, making the messages easier to receive. Messages to Scapa were never to be sent by wireless, and when the fleet was at sea, messages might be sent using lower power and relay ships (including private vessels), to make German interception more difficult. No attempts were made by the German fleet to restrict its use of wireless until 1917 and then only in response to perceived British use of direction finding, not because it believed messages were being decoded.

On 17 January 1917, Nigel de Grey, a young naval intelligence officer, hurried to the office of his wartime superior, Captain William Hall, Director of Naval Intelligence. Once inside, de Grey impatiently spluttered out his question. ‘Do you want to bring America into the war, sir?’ The short, dapper captain, known to his subordinates and colleagues as ‘Blinker’ Hall because of his rapidly blinking eyes, was immediately alert. ‘Yes, why?’ he exclaimed. De Grey brandished a piece of paper, exclaiming ‘I’ve got a telegram here that will bring them in if you give it to them’. The war was at a critical stage. A dreadful, bloody stalemate on land and sea was consuming lives at an awful rate. The military offered no obvious way of breaking the deadlock. America’s entry to the war, however, could sway the balance and bring the dreadful slaughter to an end. But neither America’s government nor its people wanted to join the Europeans’ imperial war. If de Grey was not exaggerating the import of his intelligence, then whatever it was he had discovered could be decisive in determining the outcome of the war. De Grey was one of the handful of people who worked in Room 40 of the Admiralty in central London. Their task was to break German naval and diplomatic codes.

This particular telegram had been sent from Berlin, via Washington, to the German representative in Mexico. De Grey, and a colleague Dilly Knox, had managed to make out only some passages of the message. But what they had revealed was enough to send de Grey dashing off to Hall’s office.

In the telegram the German Foreign Secretary, Arthur Zimmermann, proposed that Germany and Mexico join forces in waging war – ‘conduct war jointly; make peace jointly’ – against the United States. When the telegram’s contents were fully decoded and revealed to the American public, America was propelled into joining the war, ensuring Germany’s defeat.

This intercepted message is Room 40’s most renowned achievement. Yet, the ‘Zimmermann Telegram’ was just one of many tens of thousands of wireless and telegraph cable messages systematically intercepted throughout the war and decoded by the Room 40, and also by its little known War Office equivalent, MI1(b).

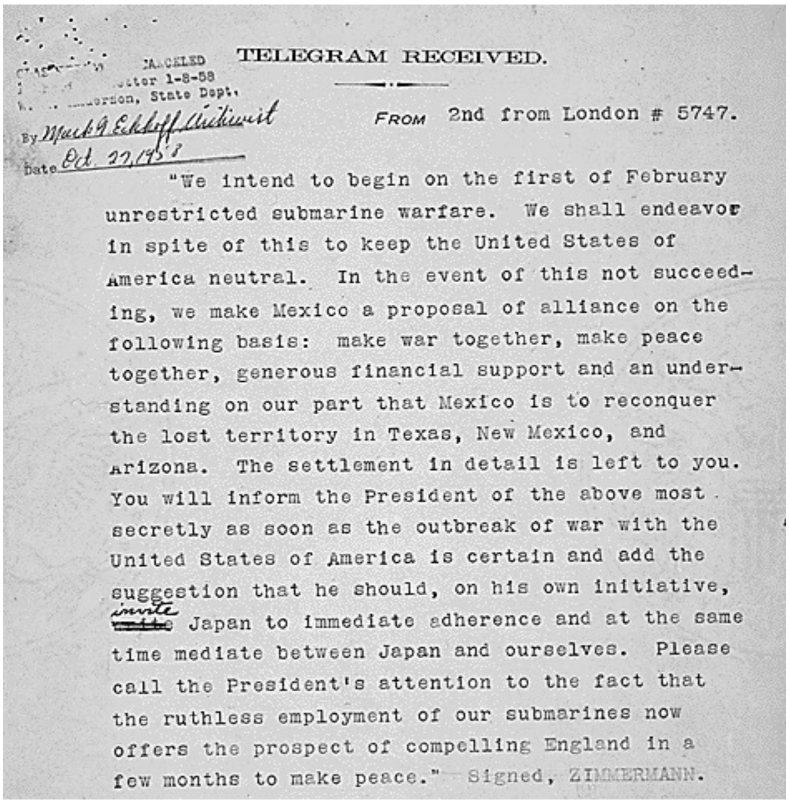
The decoded Zimmermann telegram.

British code breakers in the First World War peeped into the secret military, naval and diplomatic messages of Germany and its allies, and also into the diplomatic messages of neutrals, including the USA, Spain, the Netherlands, Greece and Switzerland. British code breaking was part of the overall effort that achieved victory. And, by bringing America into the war, code breaking was critical in determining who would be the winners and the losers.

The geographical spread and range of topics covered in those messages is astounding. They reveal how Room 40 and MI1(b) gave British military and government leaders an extraordinary oversight of their enemies’ activities on every continent and on every ocean of the land war, the sea and air war, the espionage and sabotage war, and the propaganda and diplomatic war.

The First World War was truly global, with fighting in many regions, not just the Western Front and the North Sea. Other nations had large-scale code breaking operations, but what distinguished the British effort was its systematic nature. The British had already moved to protect its globally-encompassing telegraph cable network – the 'All-Red Line' – and had curtailed German international telegraph communications by cutting five sub-sea German cables off the Atlantic coast.

At the start of the war, codes and ciphers deployed by the military, naval, and diplomatic services on all sides were relatively primitive, derived from the age of the cavalry on land and of sail at sea. There was an awareness of the need for secrecy, so signals were first encoded using common codebooks; then, for additional security, signals were enciphered. The concepts underlying these techniques, however, were distinctly old-fashioned, and also increasingly vulnerable to innovations in code-breaking techniques.



CA.CELED
...ctor 1-8-58
...erson, State Dept.
By Mark G Eckhoff Archivist
Date Oct. 22, 1958

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

The basis of Room 40 operations evolved around a German naval codebook, the *Signalbuch der Kaiserlichen Marine* (SKM), and around maps (containing coded squares), which Britain's Russian allies had passed on to the Admiralty.

The Russians had seized this material from the German cruiser SMS *Magdeburg* when it ran aground off the Estonian coast on 26 August 1914. The Russians recovered two of the four copies that the warship had carried; they retained one and passed the other to the British.

In October 1914 the British also obtained the Imperial German Navy's *Handelsschiffsverkehrsbuch* (HVB), a codebook used by German naval warships, merchantmen, naval zeppelins and U-Boats: the Royal Australian Navy seized a copy from the Australian-German steamer *Hobart* on 11 October. On 30 November a British trawler recovered a safe from the sunken German destroyer *S-119*, in which was found the *Verkehrsbuch* (VB), the code used by the Germans to communicate with naval attachés, embassies and warships overseas.

In March 1915 a British detachment impounded the luggage of Wilhelm Wassmuss, a German agent in Persia and shipped it, unopened, to London, where the Director of Naval Intelligence, Admiral Sir William Reginald Hall discovered that it contained the German Diplomatic Code Book, Code No. 13040.

The function of the Room 40 program was compromised by the Admiralty's insistence upon interpreting Room 40 information in its own way. Room 40 operators were permitted to decrypt but not to interpret the information they acquired.

The section retained "Room 40" as its informal name even though it expanded during the war and moved into other offices. It was estimated by Westwood in 2009 that Room 40 decrypted around 15,000 German communications, the section being provided with copies of all intercepted communications traffic, including wireless and telegraph traffic. Alfred Ewing directed Room 40 until May 1917, when direct control passed to Captain (later Admiral) Reginald 'Blinker' Hall, assisted by William Milbourne James.

Capture of the SKM codebook

SMS *Magdeburg* aground off Odensholm

The first breakthrough for Room 40 came with the capture of the *Signalbuch der Kaiserlichen Marine* (SKM) from the German light cruiser SMS *Magdeburg*.

Two light cruisers, *Magdeburg* and SMS *Augsburg*, and a group of destroyers all commanded by Rear-Admiral Behring were carrying out a reconnaissance of the Gulf of Finland, when the ships became separated in fog. *Magdeburg* ran aground on the island of Odensholm off the coast of Russian-controlled Estonia.

The ship could not be re-floated so the crew was to be taken on board by the destroyer SMS *V26*. The commander,*Korvettenkapitän* Habenicht prepared to blow up the ship after it had been evacuated but the fog began to clear and two Russian cruisers *Pallada* and *Bogatyr* approached and opened fire. The demolition charges were set off prematurely, causing injuries amongst the crew still on board and before secret papers could be transferred to the destroyer or disposed of. Habenicht and fifty-seven of his crew were captured by the Russians.

Exactly what happened to the papers is not clear. The ship carried more than one copy of the SKM codebook and copy number 151 was passed to the British. The German account is that most of the secret papers were thrown overboard, but the British copy was undamaged and was reportedly found in the charthouse.

The current key was also needed in order to use the codebook. A gridded chart of the Baltic, the ship's log and war diaries were all also recovered. Copies numbered 145 and 974 of the SKM were retained by the Russians while HMS *Theseus* was dispatched from Scapa Flow to Alexandrovosk in order to collect the copy offered to the British.

Although she arrived on 7 September, due to mix-ups she did not depart until 30 September and returned to Scapa with Captain Kredoff, Commander Smirnoff and the documents on 10 October. The books were formally handed over to the First Lord, Winston Churchill, on 13 October.

The SKM by itself was incomplete as a means of decoding messages, since they were normally enciphered as well as coded and those that could be understood were mostly weather reports.

Fleet paymaster C. J. E. Rotter, a German expert from the naval intelligence division, was tasked with using the SKM codebook to interpret intercepted messages, most of which decoded as nonsense since initially it was not appreciated that they were also enciphered.

An entry into solving the problem was found from a series of messages transmitted from the German Norddeich transmitter, which were all numbered sequentially and then re-enciphered. The cipher was broken, in fact broken twice as it was changed a few days after it was first solved, and a general procedure for interpreting the messages determined.

Enciphering was by a simple table, substituting one letter with another throughout all the messages. Rotter started work in mid-October but was kept apart from the other code breakers until November, after he had broken the cipher.

The intercepted messages were found to be intelligence reports on the whereabouts of allied ships. This was interesting but not vital. Russel Clarke now observed that similar coded messages were being transmitted on short-wave, but were not being intercepted because of shortages of receiving equipment, in particular the aerial.

Hunstanton was directed to stop listening to the military signals it had been intercepting and instead monitor short-wave for a test period of one weekend. The result was information about the movements of the High Seas Fleet and valuable naval intelligence. Hunstanton was permanently switched to the naval signals and as a result stopped receiving messages valuable to the military.

Navy men who had been helping the military were withdrawn to work on the naval messages, without explanation, because the new code was kept entirely secret. The result was bad feeling between the naval and military interception services and a cessation of cooperation between them, which continued into 1917.

The SKM (sometimes abbreviated SB in German documents) was the code normally used during important actions by the German fleet. It was derived from the ordinary fleet signal books used by both British and German navies, which had thousands of predetermined instructions which could be represented by simple combinations of signal flags or lamp flashes for transmission between ships.

The SKM had 34,300 instructions, each represented by a different group of three letters. A number of these reflected old-fashioned naval operations, and did not mention modern inventions such as aircraft. The signals used four symbols not present in ordinary Morse code (given the names alpha, beta, gamma and rho), which caused some confusion until all those involved in interception learnt to recognise them and use a standardised way to write them.

Ships were identified by a three-letter group beginning with a beta symbol. Messages not covered by the predetermined list could be spelled out using a substitution table for individual letters.

The sheer size of the book was one reason it could not easily be changed, and the code continued in use until summer 1916. Even then, ships at first refused to use the new codebook because the replacement was too complicated, so the *Flottenfunkspruchbuch* (FFB) did not fully replace the SKB until May 1917.

Doubts about the security of the SKB were initially raised by Behring, who reported that it was not definitely known whether *Magdeburg's* code books had been destroyed or not, and it was suggested at the court martial enquiry into the loss that books might anyway have been recovered by Russians from the clear shallow waters where the ship had grounded.

Prince Heinrich of Prussia, commander in chief of Baltic operations, wrote to the C-in-C of the High Seas Fleet, that in his view it was a certainty that secret charts had fallen into the hands of the Russians, and a probability that the codebook and key had also.

The German navy relied upon the re-enciphering process to ensure security, but the key used for this was not changed until 20 October and then not changed again for another three months.

The actual substitution table used for enciphering was produced by a mechanical device with slides and compartments for the letters. Orders to change the key were sent out by wireless, and frequently confusion during the changeover period led to messages being sent out using the new cipher and then being repeated with the old. Key changes continued to occur infrequently, only 6 times during 1915 from March to the end of the year, but then more frequently from 1916.

There was no immediate capture of the FFB codebook to help the Admiralty understand it, but instead a careful study was made of new and old messages, particularly from the Baltic, which allowed a new book to be reconstructed. Now that the system was understood, Room 40 reckoned to crack a new key within three to four days, and to have reproduced the majority of a new codebook within two months.

A German intelligence report on the matter was prepared in 1934 by *Korvettenkapitän* Kleikamp which concluded that the loss of *Magdeburg's* codebook had been disastrous, not least because no steps were taken after the loss to introduce new secure codes.

Capture of the HVB codebook

The second important code used by the German navy was captured at the very start of the war in Australia, although it did not reach the Admiralty until the end of October. The German-Australian steamer *Hobart* was seized off Port Phillip Heads near Melbourne on 11 August 1914. *Hobart* had not received news that war had broken out, and Captain J. T. Richardson and party claimed to be a quarantine inspection team.

Hobart's crew were allowed to go about the ship, but the captain was closely observed, until in the middle of the night he attempted to dispose of hidden papers. The *Handelsverkehrsbuch* (HVB) codebook which was captured contained the code used by the German navy to communicate with its merchant ships and also within the High Seas Fleet. News of the capture was not passed to London until 9 September. A copy of the book was made and sent by the fastest available steamer, arriving at the end of October.

The HVB was originally issued in 1913 to all warships with wireless, to naval commands and coastal stations. It was also given to the head offices of eighteen German steamship companies to issue to their own ships with wireless.

The code used 450,000 possible four-letter groups which allowed alternative representations of the same meaning, plus an alternate ten-letter grouping for use in cables. Re-ciphering was again used but for general purposes was more straightforward, although changed more frequently. The code was used particularly by light forces such as patrol boats, and for routine matters such as leaving and entering harbour.

The code was used by U-boats, but with a more complex key. However, the complications of their being at sea for long periods meant that codes changed while they were away and often messages had to be repeated using the old key, giving immediate information about the new one. German intelligence were aware in November 1914 that the HVB code had fallen into enemy hands, as evidenced by wireless messages sent out warning that the code was compromised, but it was not replaced until 1916.

The HVB was replaced in 1916 by the *Allgemeinefunkspruchbuch* (AFB) together with a new method of keying. The British obtained a good understanding of the new keying from test signals, before it was introduced for real messages. The new code was issued to even more organisations than the previous one, including those in Turkey, Bulgaria and Russia. It had more groups than its predecessor but now of only two letters. The first copy to be captured came from a shot-down Zeppelin but others were recovered from sunk U-boats.

Capture of the VB codebook

A third codebook was recovered following the sinking of German destroyer SMS *S119* in the Battle off Texel. In the middle of October 1914, the Battle of the Yser was fought for control of the coastal towns of Dixmude and Dunkirk. The British navy took part by bombarding German positions from the sea and German destroyers were ordered to attack the British ships.

On 17 October Captain Cecil Fox commanding the light cruiser *Undaunted* together with four destroyers, HMS *Lance*, *Lennox*, *Legion* and *Loyal*, was ordered to intercept an anticipated German attack and met four German destroyers (*S115*, *S117*, *S118*, and *S119*) heading south from Texel with instructions to lay mines.

The German ships were outclassed and all were sunk after a brief battle, whereupon the commander of *S119* threw overboard all secret papers in a lead-lined chest. The matter was dismissed by both sides, believing the papers had been destroyed along with the ships. However, on 30 November a British trawler dragged up the chest which was passed to Room 40 (Hall later claimed the vessel had been searching deliberately). It contained a copy of the *Verkehrsbuch* (VB) codebook, normally used by flag officers of the German Navy. Thereafter the event was referred to by Room 40 as "the miraculous draft of fishes".

The code consisted of 100,000 groups of 5-digit numbers, each with a particular meaning. It had been intended for use in cables sent overseas to warships and naval attachés, embassies and consulates. It was used by senior naval officers with an alternative *Lambda* key, none of which failed to explain its presence on a small destroyer at the start of the war. Its greatest importance during the war was that it allowed access to communications between naval attachés in Berlin, Madrid, Washington, Buenos Aires, Peking, and Constantinople.

In 1917 naval officers switched to a new code with a new key *Nordo* for which only 70 messages were intercepted, but the code was also broken. For other purposes VB continued in use throughout the war. Re-ciphering of the code was accomplished using a key made up of a codeword transmitted as part of the message and its date written in German.

These were written down in order and then the letters in this key were each numbered according to their order of appearance in the alphabet. This now produced a set of numbered columns in an apparently random order. The coded message would be written out below these boxes starting top left and continuing down the page once a row was filled. The final message was produced by taking the column numbered '1' and reading off its contents downward, then adding on the second column's digits, and so on.

In 1918 the key was changed by using the keywords in a different order. This new cipher was broken within a few days by Professor Walter Horace Bruford, who had started working for Room 40 in 1917 and specialised in VB messages. Two messages were received of identical length, one in the new system and one in the old, allowing the changes to be compared.

The main German naval codebook, called the Imperial Navy Signal Book ('Signalbuch der Kaiserlichenmarine'), treated coding methods for wireless signals as an afterthought, added onto a publication that concentrated on traditional means of signalling at sea, i.e., using flags and other visual techniques, such as flashes of light.

The design of this and the other codebooks used by the Imperial German Navy and German Army was simple in the extreme. The codebooks listed plain words alphabetically, but also allocated code words in alphabetic order, thus making the coded signals very vulnerable to the code breakers, even if they did not have direct access to the codebooks being used.

In any event, British Admiralty code breakers working in Room 40 did not have to concern themselves initially with cracking the codebook structures: this was because all three of the main German naval codebooks were captured within a few months of the start of hostilities

Similarly, the cipher techniques, used to 'super-encipher' the coded signals, they found were surprisingly primitive. In some cases they even used the simple 'Caesar Cipher', where there is a fixed transposition of one letter in the alphabet for another (so coded letter A is always transposed to enciphered letter D, for instance). These ciphers, even if slightly more sophisticated, were an easy technique to break.

So, it was no surprise that French and British army code breakers worked-out how to crack German army cipher techniques in the short period of mobile warfare up to the First Battle of the Marne (September 1914). This was to prove fortunate as, once the trenches had been dug and cables laid, the German Army used very little wireless signalling on the Western Front until later in the war. Information about this valuable technique was passed back to Room 40, which was then able to decipher all German naval wireless traffic.

For some time into the conflict, even when the German codebooks were replaced with new versions, they were structured in the same way using the same alphabetical plain word/codeword allocations, and thus took little time to break. Similarly, although the German forces changed their individual cipher keys fairly regularly, they stuck for two-to-three years with the same simple cipher systems, and it took some time for new keys to be broken by the British.

From August 1914 the British Royal Navy thus had an unmatched insight into the activities of its German counterpart, listening-in to instructions for enemy vessels to collect at a certain time, and for harbour lights to be turned on at the same time (thus revealing that the Imperial German Navy battle fleet was preparing to set to sea on a sortie): one of these led to the Battle of Jutland (30 May-1 June 1916).

Room 40's intelligence gathering was aided by the prolific use of wireless communications by the German Navy, with submarines and small surface vessels such as minesweepers, announcing departure, course and activities at frequent intervals. To be sure, this harvest of prime intelligence was not always used to best advantage by the Royal Navy's admirals and commanders. The Battle of Jutland was effective by default, in that it scared the Imperial German Navy surface fleet into remaining in port for the remainder of the First World War – but the Royal Navy missed the opportunity to hammer its enemy's fleet. Indeed, it took a good two years for the Admiralty to understand how best to organise Room 40's operations effectively.

Contrary to expectations Room 40 founder, engineer and physicist Sir James Alfred Ewing, turned out to be not a particularly good leader of an operational unit, and in 1917 was replaced by the more dynamic (and devious) Captain (later Admiral Sir) William Reginald Hall (1870-1943), the director of Naval Intelligence from 1914 to 1919 (who was known as 'Blinker' Hall due to a facial twitch, which reportedly caused one of his eyes to blink like a flashing Navy signal lamp).

Progress in terms of intelligence gathering and processing was patchy on land, too, in the early years of the conflict. The opposing armies, bogged down in the trenches, laid-out dense networks of communications cables, rather than use wireless communications at the front. Both sides also learnt how to 'tap' into their enemies' telephone and telegraph communications; but ironically, they did not always pay sufficient attention to securing their own communications.

Arguably, the most important development in British code breaking at this stage of the war was the way code breakers British Military Intelligence (MI1b for the army, Room 40 for the Royal Navy) turned their attention to diplomatic eavesdropping. They began to take an interest not just in German diplomatic communications, but even those of friendly neutral nations, such as the USA.

The US diplomatic codebook was broken by a sound, if unoriginal, ruse. The British handed the US ambassador in London a diplomatic note that they knew would have to be transmitted by telegraph to Washington in full. Before crossing the ocean on a submarine cable, the now encoded message was sent on a telegraph land cable from London to Cornwall. The British were able to covertly intercept the signal en-route to the West Country, and used it to start working-out the structure of the US code scheme.

This allowed the British military and political leaders to follow US diplomatic moves, such as the promotion of peace talks, and to keep tabs on Germany's efforts to coerce neutrals into supporting its point-of-view before it introduced unrestricted submarine warfare at the beginning of 1917. The codebooks used by that time were much more complex than the early alphabetic allocation codebooks. Code words were now allocated randomly, making it much more difficult to break new codebooks if a physical copy had not already been captured.

It was necessary to work-out about half of the codeword meanings of a codebook before it would be practical to break enough of the individual messages to make any sense of them. It would take a lot of effort, therefore, to break a codebook with 10,000 code words – which was not an unusual number at the time.

As the First World War progressed the Germans changed their codebooks more frequently, so it was necessary to break a book quite quickly – or all the effort would be wasted when a new one was introduced. The code breakers would use complex logical assumptions to identify, first, code words representing numbers, punctuation and common terms such as names, units, call signs, and suchlike. From then they could start to focus-in on more and more of the content of coded messages. It was a slow and arduous process, and needed people who worked with words – such as professional lexicographers, experts in ancient history, and other specialist linguists – whereas, by contrast, in the Second World War ciphers needed mathematicians.

Code breaking was a very labour-intensive process, and the volumes of data being collected was soon placing strain on the Room 40 team and its resources (an Allied intelligence report of 1918 notes that code breakers "must possess the faculty of keeping anything from a dozen to 20 theories in their minds in order to build-up a chain of coincidence and reasoning until each link fits into its place and forms a coherent whole".

Sometime in 1916 one of their number came-up with the idea of using machinery to work out the sequence of logical steps of the code-breaking process, usually known as 'flow-charting'. The science of code breaking and interpreting intelligence was about to enter a new and highly significant phase that would, it can be argued, result in innovations that would play into the development of the electronic computer, leading to Bletchley Park's Colossus.

Not much hard evidence about the nature of the Room 40 apparatus, or how it functioned, survives. Whatever physical form it took, it was almost certainly a type of punched card tabulator machine. The tabulating machine was an electromechanical machine invented to help summarise fielded information and, later, accounting applications; computing giant IBM had its origins in tabulating machine technology.

The only clue about the Room 40 hardware is mention of a 'pianola'. It was quite common for the pianola-type device to be mentioned in a description/introduction to the idea of punched card machinery in computer histories (pianolas are sometimes described as among the first example of mechanical automation). The key point is the 'holes/not holes' concept as a means of conveying machine commands and/or information, rather than the precise nature of the card/ roll.

The code breakers adopted the term 'hatted' for these randomly allocated codebooks, as if the codeword for any plain word had been drawn out of a hat. This led to the description of the team of machine operating women as 'grinding' codeword meanings 'out of the hat machine'.

There is, however, some information about how the new Room 40 machinery sped-up the process of working out code words. In a document about diplomatic code breaking there is a short account of the project: "It was not realised that this form of [randomly allocated] code required special treatment until May 1916 when leave was granted to set-up a special staff of educated women to work machinery by which the guessing process could be accelerated... By this method the [number of] guessed code words rose at once to 20 daily, and by the law of increasing returns grew mechanically to a maximum of 100 per day by which time the code was approximately readable."

This contrasted with a handful of code words that could be worked-out in a day by a practiced person. It is the sort of productivity increase that we typically associate with the introduction of modern information technology (IT) to a data-processing-intensive requirement. In another indication of the way that IT changes the nature of work, the report adds that "the reading of messages in such codes proved to be merely a matter of tedious drudgery for one or two experts and the staff of ladies trained by Miss Robertson".

Knowledge of its existence helps us understand why Second World War code breaking machines such as Colossus (and many other less-well-known machines) were invented at Bletchley Park. The concept of using machines for code breaking was not new in 1940, but was yet another way in which the First World War forerunners helped define the progress of the later conflict.

Most sensationally, Room 40 intercepted a January 1917 cable message from the German foreign minister, Arthur Zimmermann, which attempted to bring Mexico into the war on Germany's side by militarily attacking the United States. The cable was decoded, and its contents leaked to the US President: it played a part in bringing the US into the war, tipping the balance of power against Germany and its allies. The incident has gone down in cryptographic history as the interception of the 'Zimmermann Telegram'.

It was a triumph for the eavesdroppers and the code breakers, but also for William Hall, who worked-out how to pass the intelligence onto the Americans while retaining two important secrets. The first secret was to make sure that the Germans did not realise that Britain was intercepting and decoding their secret communications; this was militarily vital. Fortunately, the Germans blamed their own people, not the enemy, for the leak, so this secret was safe. It was also politically vital that a second secret also be held very securely indeed. This time it was the Americans who had to be kept in the dark.

US President Woodrow Wilson had allowed the Germans to bundle their cables in with those ostensibly coming from the US embassy in Copenhagen, Denmark. The reason for this was that, as previously mentioned, the British had cut Germany's cables and had captured its international wireless stations, gaining a hold on its communications with the wider world. President Wilson allowed Germany to use US facilities to communicate with the German Embassy in Washington, supposedly about his peace proposals. Instead, Zimmermann used the channel to try and provoke a wider war that included an attack on the US mainland.

Much as they would want to apprise the Americans of this diplomatic skulduggery, the British could not at the same time easily admit that they were intercepting and looking at US messages passing through British telegraph networks (which is how messages from Copenhagen were routed). Fortunately, the message had to be sent on to the German legation in Mexico City, and the British managed to spirit away a copy of the message on its arrival there – which was then shown to the American authorities.

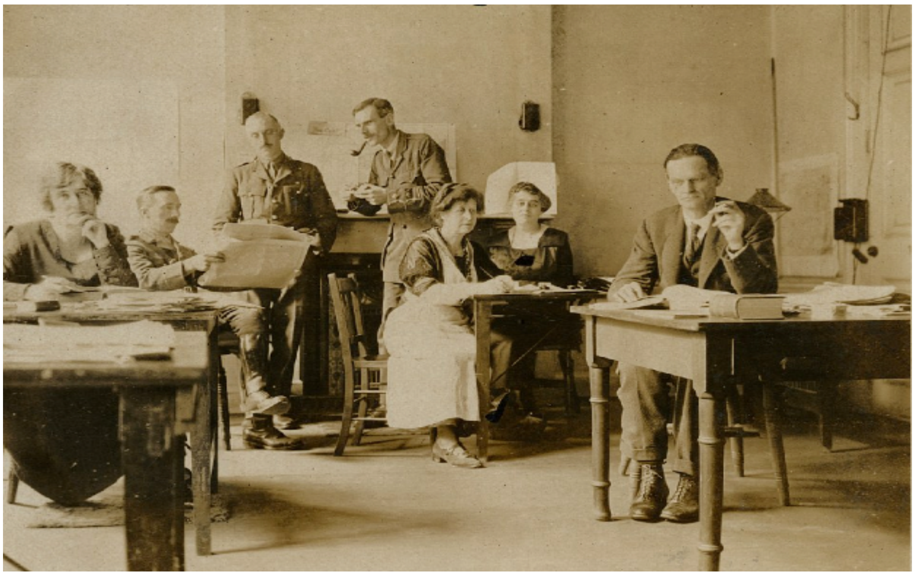
In 1917, Gilbert Vernam proposed a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cyphertext. This led to the development of electromechanical devices as cipher machines, and to the only unbreakable cipher, the one time pad.

How did the British code breakers succeed in cracking the apparently unbreakable Enigma code during the Second World War? Was it their gifted amateurism? The brilliance of Alan Turing? The invention of the very first computers? Or the pioneering work of Polish cryptographers? It was all of the above. But there is one other crucial factor, which is much less well known. The same team had done it before.

The truth is that many of those most closely involved in cracking the Enigma code – Alistair Denniston, Frank Birch, Dilly Knox – had wrestled with German naval codes for most of the First World War. By the end of the war they had been successfully cracking a new code every day, from their secret Room 40 at the Old Admiralty Building, in a London blacked out for Zeppelin Raids.

The techniques they developed then, the ideas that they came to rely on, the people they came to trust, had been developed the hard way, under intense pressure and absolute secrecy during World War I. Before Enigma tells their story and explains how they managed to crack the supposedly indecipherable code.

After the Armistice in 1918 Room 40's necessity waned. Other staff of Room 40 included Frank Adcock, John Beazley, Francis Birch, Walter Horace Bruford, William 'Nobby' Clarke, Alastair Denniston, Frank Cyril Tiarks and Dilly Knox. In 1919, Room 40 was deactivated and its function merged with the British Army's intelligence unit MI1b to form the Government Code and Cypher School (GC&CS).



The First Bletchley Park: This incredible image taken in June 1919 shows World War One code breakers - including Major Malcolm Hay (back left) in their secret office in London. The organisation, known as Room 40, had a pivotal role in bringing the Great War to an end.

This grainy image, taken in August 1919, shows some of those who worked at the organisation. The photo is taken from an album which was presented to Sir Malcolm, staff to the director, when he retired.

According to annotations on the photograph, this image features Mr Phillipson Stour, Captain DH Lindsay, Mr Maine, Major Hay and Captain Brooke Hunt

One of the legendary code breakers in Room 40 was Dillwyn 'Dilly' Knox, a classical scholar who liked to work while sat in a hot bath - and once cracked one of the most important codes during a long soak.

Alfred Dillwyn 'Dilly' Knox was a classics scholar and British eccentric who became an integral part of the codebreaking unit during both of the world wars.With some of his best work said to have been carried out in the bath, Dilly helped to decrypt the Zimmerman Telegram, which brought the US into the war. At the end of the war, he joined Government Code and Cypher School at Bletchley Park as chief cryptographer.He then worked on cracking the Enigma machines until his death in 1943, particularly working on the Abwehr, the German secret service which existed between 1920 to 1945.

Thanks to Knox's team, British intelligence was able to monitor Abwehr activities and even plant false information – something that would later prove critical to the success of D-Day. By the end of the war, Knox had disseminated 140,800 Abwehr codes.

Surviving records from Room 40, including a neatly-typed record of who paid what into the tea kitty. The document, from September 24, 1917, shows how Oliver Strachey gave 5 shillings and 2 pence while Captain Brooke Hunt gave £1 2s.

The exhibition also republishes a unique parody of Alice's Adventures in Wonderland, created at Room 40, which poked fun at the wartime work of the codebreakers. Originally written by Knox and his colleague Frank Birch at the end of World War One, it was performed privately as a pantomime in London in December 1918. The parody described life in Room 40 and the people who worked there and remained under wraps for many decades afterwards.

After the Treaty of Versailles in 1919, the German defence establishment was eager to improve its compromised communications system, and recognised the potential of a signalling device that had originally been made for the business market.

Dr Arthur Scherbius had developed his 'Enigma' machine, capable of transcribing coded information, in the hope of interesting commercial companies in secure communications. In 1923 he set up his Chiffriermaschinen Aktiengesellschaft (Cipher Machines Corporation) in Berlin to manufacture this product, and within three years the German navy was producing its own version, followed in 1928 by the army and in 1933 by the air force.

Enigma allowed an operator to type in a message, then scramble it by means of three to five notched wheels, or rotors, which displayed different letters of the alphabet. The receiver needed to know the exact settings of these rotors in order to reconstitute the coded text. Over the years the basic machine became more complicated, as German code experts added plugs with electronic circuits.

It was only after they had handed over details to the Polish Cipher Bureau that progress was made. Helped by its closer links to the German engineering industry, the Poles managed to reconstruct an Enigma machine, complete with internal wiring, and to read the Wehrmacht's messages between 1933 and 1938.

Alfred Dillwyn "Dilly" Knox, CMG (23 July 1884 – 27 February 1943) was a British classics scholar and Papyrologist at King's College, Cambridge and a code breaker. As a member of the World War I Room 40 codebreaking unit, he helped decrypt the Zimmermann Telegram which brought the USA into World War I.